COTS Security Workgroup
Special Tasking
February 5, 2003

Background

In the event of war, terrorist attacks, cyber attacks, or other natural or man-made catastrophic occurrences in the Commonwealth of Virginia, coordinated contingency plans are necessary to respond to and recover from emergencies that impact technology infrastructure and services.

Task

The Council on Technology Services (COTS) Security Workgroup shall develop coordinated contingency plans and procedures to protect and restore the Commonwealth's critical technology services and infrastructure, and shall take into account a wide range of potential cyber security events, from a computer virus attack to decimation of entire regions of the Commonwealth. These plans will include the notification of technology personnel of an event, coordinated operations plans to effect recovery of critical services, and post-event plans to resume normal operations. This task takes priority over the existing work being done by the Workgroup.

Approach

Given the likelihood of war and further attacks on American interests, the need for these plans and procedures is urgent and, therefore, should be completed in a time-phased approach, as follows:

30 Days: Seek assistance from James Madison University and the alliance of colleges and universities working on security and homeland security issues.

Develop an enterprise-wide notification system to alert agency personnel of cybersecurity incidents.

Review existing policies, plans, and procedures and begin process of identifying threats in order of likelihood.

60 Days Develop recommendations for near- and long-term actions and strategies that the Commonwealth needs to take.

90 Days Develop recommendations for enterprise contingency plans for the Commonwealth Enterprise Security office that is planned within the Virginia Information Technologies Agency (VITA).

Develop a "scorecard" for measuring by agency or by Secretariat existing policies, plans, and procedures for preventing, responding to, or recovering from a cybersecurity incident.

The COTS Security Workgroup shall work in tandem with the Technology Sub-Panel of the Secure Virginia Initiative Panel. It is assumed that disaster recovery and business continuity plans for the Executive Branch agencies will be made available from the Office of Commonwealth Preparedness to COTS Security Workgroup members who have signed a non-disclosure/confidentiality agreement. The COTS Security Workgroup shall observe the public meeting requirements of the Freedom of Information Act, and shall follow the procedures for convening in Closed Session when confidential or sensitive information is under discussion.